U.S. Patent Application Serial No. 09/889,918
Reply to Office Action dated May 16, 2006

Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the

application:

Listing of Claims:

1 - 19. (Cancelled)

20.   (Currently Amended) A ~~The~~ computer implemented process ~~according to claim 19,~~

~~further~~ comprising:

obtaining a set of one or more private values $Q_1, Q_2, ..., Q_m$ and respective public values

$G_1, G_2, ..., G_m$, each pair of values Q_i, G_i verifying either the equation $G_i \cdot Q_i^v \equiv 1 \bmod n$ or the

equation $G_i \equiv Q_i^v \bmod n$, wherein m is an integer greater than or equal to 1, i is an integer

between 1 and m, and wherein n is a public integer equal to the product of f private prime

factors designated by $p_1, ..., p_f$, at least two of these prime factors being different from each

other, wherein f is an integer greater than 1, and wherein v is a public exponent such that

$v = 2^k$, and wherein k is a security parameter having an integer value greater than 1, and

wherein each public value G_i for $i = 1, ..., m$ is such that $G_i \equiv g_i^2 \bmod n$, wherein g_i for

$i = 1, ..., m$) is a base number having an integer value greater than 1 and smaller than each of the

prime factors $p_1, ..., p_f$, and g_i is a non-quadratic residue of the ring of integers modulo n;

receiving a commitment R from a demonstrator, the commitment R having a value

computed such that: $R = r^v \bmod n$, wherein r is an integer randomly chosen by the

demonstrator;

2

choosing m challenges $d_1, d_2, ..., d_m$ randomly;

sending the challenges $d_1, d_2, ..., d_m$ to the demonstrator;

receiving a response D from the demonstrator, the response D having a value computed

such that: ~~$D = r \times Q_1^{d_1} \times Q_2^{d_2} \times ... \times Q_m^{d_m} \bmod n$~~; $\underline{D = r \bullet Q_1^{d_1} \bullet Q_2^{d_2} \bullet ... \bullet Q_m^{d_m} \bmod n}$;and

determining that the demonstrator is authentic if the response D has a value such that:

~~$D^v \times G_1^{\varepsilon_1 d_1} \times G_2^{\varepsilon_2 d_2} \times ... \times G_m^{\varepsilon_m d_m} \bmod n$~~ $\underline{D^v \bullet G_1^{\varepsilon_1 d_1} \bullet G_2^{\varepsilon_2 d_2} \bullet ... \bullet G_m^{\varepsilon_m d_m} \bmod n}$ is equal to the

commitment R, wherein, for $i = 1, ..., m$, $\varepsilon_i = +1$ in the case ~~$G_i \times Q_i^v = 1 \bmod n$~~

$\underline{G_i \bullet Q_i^v = 1 \bmod n}$ and $\varepsilon_i = -1$ in the case $\underline{G_i = Q_i^v \bmod n}$.

21.   (Currently Amended) $\underline{A}$ ~~The~~ computer implemented process ~~according to claim 19,~~ ~~further~~ comprising:

$\underline{\text{obtaining a set of one or more private values } Q_1, Q_2, ..., Q_m \text{ and respective public values}}$

$\underline{G_1, G_2, ..., G_m, \text{ each pair of values } Q_i, G_i \text{ verifying either the equation } G_i \cdot Q_i^v \equiv 1 \bmod n \text{ or the}}$

$\underline{\text{equation } G_i \equiv Q_i^v \bmod n, \text{ wherein } m \text{ is an integer greater than or equal to } 1, i \text{ is an integer}}$

$\underline{\text{between 1 and } m, \text{ and wherein } n \text{ is a public integer equal to the product of } f \text{ private prime}}$

$\underline{\text{factors designated by } p_1, ..., p_f, \text{ at least two of these prime factors being different from each}}$

$\underline{\text{other, wherein } f \text{ is an integer greater than 1, and wherein } v \text{ is a public exponent such that}}$

$\underline{v = 2^k, \text{ and wherein } k \text{ is a security parameter having an integer value greater than 1, and}}$

$\underline{\text{wherein each public value } G_i \text{ for } i = 1, ..., m \text{ is such that } G_i \equiv g_i^2 \bmod n, \text{ wherein } g_i \text{ for}}$

3

$i=1,...,m$ is a base number having an integer value greater than 1 and smaller than each of the prime factors $p_1,...,p_f$, and g_i is a non-quadratic residue of the ring of integers modulo n;

receiving a commitment R from a demonstrator, the commitment R having a value computed using the Chinese remainder method from a series of commitment components R_j, the commitment components R_j having a value such that: $R_j = r_j^v \bmod p_j$ for $j=1,...,f$, wherein $r_1,...,r_f$ is a series of integers randomly chosen by the demonstrator;

choosing m challenges $d_1, d_2,...,d_m$ randomly;

sending the challenges $d_1, d_2,...,d_m$ to the demonstrator;

receiving a response D from the demonstrator, the response D being computed from a series of response components D_j using the Chinese remainder method, the response components D_j having a value such that: $\cancel{D_j = r_j \times Q_{1,j}^{d_1} \times Q_{2,j}^{d_2} \times ... \times Q_{m,j}^{d_m} \bmod p_j}$

$\underline{D_j = r_j \bullet Q_{1,j}^{d_1} \bullet Q_{2,j}^{d_2} \bullet ... \bullet Q_{m,j}^{d_m} \bmod p_j}$ for $j=1,...,f$, wherein $Q_{i,j} = Q_i \bmod p_j$ for $i=1,...,m$ and $j=1,...,f$; and

determining that the demonstrator is authentic if the response D has a value such that: $\cancel{D^v \times G_1^{\varepsilon_1 d_1} \times G_2^{\varepsilon_2 d_2} \times ... \times G_m^{\varepsilon_m d_m} \bmod n}$ $\underline{D^v \bullet G_1^{\varepsilon_1 d_1} \bullet G_2^{\varepsilon_2 d_2} \bullet ... \bullet G_m^{\varepsilon_m d_m}}$ mod n is equal to the commitment R, wherein, for $i=1,...,m$, $\varepsilon_i = +1$ in the case $\cancel{G_i \times Q_i^v = 1 \bmod n}$ $\underline{G_i \bullet Q_i^v = 1 \bmod n}$ and $\varepsilon_i = -1$ in the case $G_i = Q_i^v \bmod n$.

22.   (Currently Amended) A ~~The~~ computer implemented process ~~according to claim 19, further~~ comprising:

4

obtaining a set of one or more private values $Q_1, Q_2, ..., Q_m$ and respective public values $G_1, G_2, ..., G_m$, each pair of values Q_i, G_i verifying either the equation $G_i \cdot Q_i^v \equiv 1 \bmod n$ or the equation $G_i \equiv Q_i^v \bmod n$, wherein m is an integer greater than or equal to 1, i is an integer between 1 and m, and wherein n is a public integer equal to the product of f private prime factors designated by $p_1, ..., p_f$, at least two of these prime factors being different from each other, wherein f is an integer greater than 1, and wherein v is a public exponent such that $v = 2^k$, and wherein k is a security parameter having an integer value greater than 1, and wherein each public value G_i for $i = 1, ..., m$ is such that $G_i \equiv g_i^2 \bmod n$, wherein g_i for $i = 1, ..., m$ is a base number having an integer value greater than 1 and smaller than each of the prime factors $p_1, ..., p_f$, and g_i is a non-quadratic residue of the ring of integers modulo n;

receiving a token T from a demonstrator, the token T having a value such that $T = h(M, R)$, wherein h is a hash function, M is a message received from the demonstrator, and R is a commitment having a value computed such that: $R = r^v \bmod n$, wherein r is an integer randomly chosen by the demonstrator;

choosing m challenges $d_1, d_2, ..., d_m$ randomly;

sending the challenges $d_1, d_2, ..., d_m$ to the demonstrator;

receiving a response D from the demonstrator, the response D having a value such that: $\cancel{D = r \times Q_1^{d_1} \times Q_2^{d_2} \times ... \times Q_m^{d_m} \bmod n}$; $D = r \bullet Q_1^{d_1} \bullet Q_2^{d_2} \bullet ... \bullet Q_m^{d_m} \bmod n$; and

determining that the message M is authentic if the response D has a value such that: $\cancel{h(M, D^v \times G_1^{c_1 d_1} \times G_2^{c_2 d_2} \times ... \times G_m^{c_m d_m} \bmod n)}$ $h(M, D^v \bullet G_1^{c_1 d_1} \bullet G_2^{c_2 d_2} \bullet ... \bullet G_m^{c_m d_m} \bmod n)$ is equal

5

to the token T, wherein, for $i = 1,...,m$, $\varepsilon_i = +1$ in the case $\cancel{G_i \times Q_i^v = 1 \bmod n}$

$G_i \bullet Q_i^v = 1 \bmod n$ and $\varepsilon_i = -1$ in the case $G_i = Q_i^v \bmod n$.

23.   (Currently Amended) A ~~The~~ computer implemented process ~~according to claim 19,~~ ~~further~~ comprising:

obtaining a set of one or more private values $Q_1, Q_2,...,Q_m$ and respective public

values $G_1, G_2,...,G_m$, each pair of values Q_i, G_i verifying either the equation $G_i \cdot Q_i^v \equiv 1 \bmod n$ or

the equation $G_i \equiv Q_i^v \bmod n$, wherein m is an integer greater than or equal to 1, i is an integer

between 1 and m, and wherein n is a public integer equal to the product of f private prime

factors designated by $p_1,...,p_f$, at least two of these prime factors being different from each

other, wherein f is an integer greater than 1, and wherein v is a public exponent such that

$v = 2^k$, and wherein k is a security parameter having an integer value greater than 1, and

wherein each public value G_i for $i = 1,...,m$ is such that $G_i \equiv g_i^2 \bmod n$, wherein g, for $i = 1,...,m$

is a base number having an integer value greater than 1 and smaller than each of the prime

factors $p_1,...,p_f$, and g_i is a non-quadratic residue of the ring of integers modulo n:

receiving a token T from a demonstrator, the token T having a value such that

$T = h(M,R)$, wherein h is a hash function, M is a message received from the demonstrator,

and R is a commitment having a value computed out of commitment components R_j by using

the Chinese remainder method, the commitment components R_j having a value such that:

6

$R_j = r_j{}^{v} \bmod p_j$ for $j = 1, \ldots, f$, wherein $r_1, \ldots, r_l$ is a series of integers randomly chosen by the demonstrator;

choosing m challenges $d_1, d_2, \ldots, d_m$ randomly;

sending the challenges $d_1, d_2, \ldots, d_m$ to the demonstrator;

receiving a response D from the demonstrator, the response D being computed from a series of response components D_j using the Chinese remainder method, the response components D_j having a value such that: ~~$D_j = r_j \times Q_{1,j}{}^{d_1} \times Q_{2,j}{}^{d_2} \times \ldots \times Q_{m,j}{}^{d_m} \bmod p_j$~~

$\underline{D_j = r_j \bullet Q_{1,j}{}^{d_1} \bullet Q_{2,j}{}^{d_2} \bullet \ldots \bullet Q_{m,j}{}^{d_m} \bmod p_j}$ for $j = 1, \ldots, f$, wherein $Q_{i,j} = Q_i \bmod p_j$ for

$i = 1, \ldots, m$ and $j = 1, \ldots, f$; and

determining that the message M is authentic if the response D has a value such that: ~~$h\left(M, D^v \times G_1{}^{\varepsilon_1 d_1} \times G_2{}^{\varepsilon_2 d_2} \times \ldots \times G_m{}^{\varepsilon_m d_m} \bmod n\right)$~~ $\underline{h\left(M, D^v \bullet G_1{}^{\varepsilon_1 d_1} \bullet G_2{}^{\varepsilon_2 d_2} \bullet \ldots \bullet G_m{}^{\varepsilon_m d_m} \bmod n\right)}$ is equal

to the token T, wherein, for $i = 1, \ldots, m$, $\varepsilon_i = +1$ in the case ~~$G_i \times Q_i{}^{v} = 1 \bmod n$~~

$\underline{G_i \bullet Q_i{}^{v} = 1 \bmod n}$ and $\varepsilon_i = -1$ in the case $G_i = Q_i{}^{v} \bmod n$.

24.   (Currently Amended) The <u>computer implemented</u> process according to claim 20, wherein the challenges are such that $0 \leq d_i \leq 2^k - 1$ for $i = 1, \ldots, m$.

25.   (Previously presented) <u>A</u> ~~The~~ computer implemented process ~~according to claim 19,~~ ~~further~~ comprising:

<u>obtaining a set of one or more private values $Q_1, Q_2, \ldots, Q_m$ and respective public</u>

<u>values $G_1, G_2, \ldots, G_m$, each pair of values Q_i, G_i, verifying either the equation $G_i \cdot Q_i{}^{v} = 1 \bmod n$ or</u>

the equation $G_i \equiv Q_i^v \bmod n$, wherein m is an integer greater than or equal to 1, i is an integer

between 1 and m, and wherein n is a public integer equal to the product of f private prime

factors designated by $p_1, ..., p_f$, at least two of these prime factors being different from each

other, wherein f is an integer greater than 1, and wherein v is a public exponent such that

$v = 2^k$, and wherein k is a security parameter having an integer value greater than 1, and

wherein each public value G_i for $i = 1, ..., m$ is such that $G_i \equiv g_i^2 \bmod n$, wherein g_i for

$i = 1, ..., m$ is a base number having an integer value greater than 1 and smaller than each of the

prime factors $p_1, ..., p_f$, and g_i is a non-quadratic residue of the ring of integers modulo n;

recording a message M to be signed;

choosing m integers r_i randomly, wherein i is an integer between 1 and m;

computing commitments R_i having a value such that: $R_i = r_i^v \bmod n$ for $i = 1, ..., m$;

computing a token T having a value such that $T = h(M, R_1, R_2, ..., R_m)$, wherein h is a

hash function producing a binary train consisting of m bits;

identifying the bits $d_1, d_2, ..., d_m$ of the token T; and

computing responses ~~$D_i = r_i \times Q_i^d \bmod n$~~ $D_i = r_i \cdot Q_i^{d_i} \bmod n$ for $i = 1, ..., m$.

26.   (Currently amended) The ~~process of~~ computer implemented process according to claim

25, further comprising:

collecting the token T and the responses D_i for $i = 1, ..., m$; and

8

determining that the message M is authentic if the response D has a value such that:

$$h\left(M, D^{v} \times G_{1}^{\varepsilon_1 d_1} \times G_{2}^{\varepsilon_2 d_2} \times ... \times G_{m}^{\varepsilon_m d_m} \mod n\right)$$

$$h\left(M, D_{1}^{v} \cdot G_{1}^{\varepsilon_1 d_1} \mod, D_{2}^{v} \cdot G_{2}^{\varepsilon_2 d_2} \mod n, ..., D_{m}^{v} \cdot G_{m}^{\varepsilon_m d_m} \mod n\right)$$

is equal to the token T, wherein, for $i = 1, ..., m$, $\varepsilon_i = +1$ in the case $\overline{G_i \times Q_i^v = 1 \mod n}$

$G_i \cdot Q_i^v = 1 \mod n$ and $\varepsilon_i = -1$ in the case $G_i = Q_i^v \mod n$.

27-28. (Cancelled)

29. (New) The computer implemented process according to claim 21, wherein the challenges are such that $0 \le d_i \le 2^k - 1$ for $i = 1, ..., m$.

30. (New) The computer implemented process according to claim 22, wherein the challenges are such that $0 \le d_i \le 2^k - 1$ for $i = 1, ..., m$.

31. (New) The computer implemented process according to claim 23, wherein the challenges are such that $0 \le d_i \le 2^k - 1$ for $i = 1, ..., m$.

32. (New) A computer readable medium storing instructions which when executed cause a processor to execute the following method:

obtaining a set of one or more private values $Q_1, Q_2, ..., Q_m$ and respective public values $G_1, G_2, ..., G_m$, each pair of values Q_i, G_i verifying either the equation $G_i \cdot Q_i^v \equiv 1 \mod n$ or the equation $G_i \equiv Q_i^v \mod n$, wherein m is an integer greater than or equal to 1, i is an integer between 1 and m, and wherein n is a public integer equal to the product of f private prime factors designated by $p_1, ..., p_f$, at least two of these prime factors being different from each other, wherein f is an integer greater than 1, and wherein v is a public exponent such that $v = 2^k$, and wherein k is a security parameter having an integer value greater than 1, and

9

wherein each public value G_i for $i = 1,...,m$ is such that $G_i \equiv g_i^2 \bmod n$, wherein g_i for $i = 1,...,m$ is a base number having an integer value greater than 1 and smaller than each of the prime factors $p_1,...,p_f$, and g_i is a non-quadratic residue of the ring of integers modulo n;

receiving a commitment R from a demonstrator, the commitment R having a value computed such that: $R = r^v \bmod n$, wherein r is an integer randomly chosen by the demonstrator;

choosing m challenges $d_1, d_2,...,d_m$ randomly;

sending the challenges $d_1, d_2,...,d_m$ to the demonstrator;

receiving a response D from the demonstrator, the response D having a value computed such that: $D = r \cdot Q_1^{d_1} \cdot Q_2^{d_2} \cdot ... \cdot Q_m^{d_m} \bmod n$; and

determining that the demonstrator is authentic if the response D has a value such that: $D^v \times G_1^{\varepsilon_1 d_1} \times G_2^{\varepsilon_2 d_2} \times ... \times G_m^{\varepsilon_m d_m} \bmod n$ is equal to the commitment R, wherein, for $i = 1,...,m$, $\varepsilon_i = +1$ in the case $G_i \times Q_i^v = 1 \bmod n$ and $\varepsilon_i = -1$ in the case $G_i = Q_i^v \bmod n$.

33.   (New) A computer readable medium storing instructions which when executed cause a processor to execute the following method:

obtaining a set of one or more private values $Q_1, Q_2,...,Q_m$ and respective public values $G_1, G_2,...,G_m$, each pair of values Q_i, G_i verifying either the equation $G_i \cdot Q_i^v \equiv 1 \bmod n$ or the equation $G_i \equiv Q_i^v \bmod n$, wherein m is an integer greater than or equal to 1, i is an integer between 1 and m, and wherein n is a public integer equal to the product of f private prime factors designated by $p_1,...,p_f$, at least two of these prime factors being different from each other, wherein f is an integer greater than 1, and wherein v is a public exponent such that

10

$v = 2^k$, and wherein k is a security parameter having an integer value greater than 1, and wherein each public value G_i for $i = 1,...,m$ is such that $G_i \equiv g_i^2 \mod n$, wherein g_i for $i = 1,...,m$ is a base number having an integer value greater than 1 and smaller than each of the prime factors $p_1,...,p_f$, and g_i is a non-quadratic residue of the ring of integers modulo n;

receiving a commitment R from a demonstrator, the commitment R having a value computed using the Chinese remainder method from a series of commitment components R_j, the commitment components R_j having a value such that: $R_j = r_j^v \mod p_j$ for $j = 1,...,f$, wherein $r_1,...,r_f$ is a series of integers randomly chosen by the demonstrator;

choosing m challenges $d_1, d_2,...,d_m$ randomly;

sending the challenges $d_1, d_2,...,d_m$ to the demonstrator;

receiving a response D from the demonstrator, the response D being computed from a series of response components D_j using the Chinese remainder method, the response components D_j having a value such that: $D_j = r_j \cdot Q_{1,j}^{d_1} \cdot Q_{2,j}^{d_2} \cdot .... \cdot Q_{m,j}^{d_m} \mod p_j$ for $j = 1,...,f$, wherein $Q_{i,j} = Q_i \mod p_j$ for $i = 1,...,m$ and $j = 1,...,f$; and

determining that the demonstrator is authentic if the response D has a value such that: $D^v \cdot G_1^{\varepsilon_1 d_1} \cdot G_2^{\varepsilon_2 d_2} \cdot .... \cdot G_m^{\varepsilon_m d_m} \mod n$ is equal to the commitment R, wherein, for $i = 1,...,m$, $\varepsilon_i = +1$ in the case $G_i \cdot Q_i^v = 1 \mod n$ and $\varepsilon_i = -1$ in the case $G_i = Q_i^v \mod n$.

34.   (New) A computer readable medium storing instructions which when executed cause a processor to execute the following method:

11

obtaining a set of one or more private values $Q_1, Q_2, ..., Q_m$ and respective public values

$G_1, G_2, ..., G_m$, each pair of values Q_i, G_i verifying either the equation $G_i \cdot Q_i^v \equiv 1 \bmod n$ or the

equation $G_i \equiv Q_i^v \bmod n$, wherein m is an integer greater than or equal to 1, i is an integer

between 1 and m, and wherein n is a public integer equal to the product of f private prime

factors designated by $p_1, ..., p_f$, at least two of these prime factors being different from each

other, wherein f is an integer greater than 1, and wherein v is a public exponent such that

$v = 2^k$, and wherein k is a security parameter having an integer value greater than 1, and

wherein each public value G_i for $i = 1, ..., m$ is such that $G_i \equiv g_i^2 \bmod n$, wherein g_i for

$i = 1, ..., m$ is a base number having an integer value greater than 1 and smaller than each of the

prime factors $p_1, ..., p_f$, and g_i is a non-quadratic residue of the ring of integers modulo n;

receiving a token T from a demonstrator, the token T having a value such that

$T = h(M, R)$, wherein h is a hash function, M is a message received from the demonstrator,

and R is a commitment having a value computed such that: $R = r^v \bmod n$, wherein r is an

integer randomly chosen by the demonstrator;

choosing m challenges $d_1, d_2, ..., d_m$ randomly;

sending the challenges $d_1, d_2, ..., d_m$ to the demonstrator;

receiving a response D from the demonstrator, the response D having a value such that:

$D = r \cdot Q_1^{d_1} Q_2^{d_2} \cdot ... \cdot Q_m^{d_m} \bmod n$; and

determining that the message M is authentic if the response D has a value such that:

$h\left(M, D^v \cdot G_1^{\varepsilon_1 d_1} \cdot G_2^{\varepsilon_2 d_2} \cdot ... \cdot G_m^{\varepsilon_m d_m} \bmod n\right)$ is equal to the token T, wherein, for $i = 1, ..., m$,

$\varepsilon_i = +1$ in the case $G_i \cdot Q_i^v = 1 \bmod n$ and $\varepsilon_i = -1$ in the case $G_i = Q_i^v \bmod n$.

12

35.   (New) A computer readable medium storing instructions which when executed cause a processor to execute the following method:

obtaining a set of one or more private values $Q_1, Q_2, ..., Q_m$ and respective public values $G_1, G_2, ..., G_m$, each pair of values Q_i, G_i verifying either the equation $G_i \cdot Q_i^v \equiv 1 \bmod n$ or the equation $G_i \equiv Q_i^v \bmod n$, wherein m is an integer greater than or equal to 1, i is an integer between 1 and m, and wherein n is a public integer equal to the product of f private prime factors designated by $p_1, ..., p_f$, at least two of these prime factors being different from each other, wherein f is an integer greater than 1, and wherein v is a public exponent such that $v = 2^k$, and wherein k is a security parameter having an integer value greater than 1, and wherein each public value G_i for $i = 1, ..., m$ is such that $G_i \equiv g_i^2 \bmod n$, wherein g_i for $i = 1, ..., m$ is a base number having an integer value greater than 1 and smaller than each of the prime factors $p_1, ..., p_f$, and g_i is a non-quadratic residue of the ring of integers modulo n;

receiving a token T from a demonstrator, the token T having a value such that $T = h(M, R)$, wherein h is a hash function, M is a message received from the demonstrator, and R is a commitment having a value computed out of commitment components R_j by using the Chinese remainder method, the commitment components R_j having a value such that: $R_j = r_j^v \bmod p_j$ for $j = 1, ..., f$, wherein $r_1, ..., r_f$ is a series of integers randomly chosen by the demonstrator;

choosing m challenges $d_1, d_2, ..., d_m$ randomly;

sending the challenges $d_1, d_2, ..., d_m$ to the demonstrator;

13

receiving a response D from the demonstrator, the response D being computed from a series of response components D_j using the Chinese remainder method, the response components D_j having a value such that: $D_j = r_j \cdot Q_{1,j}^{d_1} \cdot Q_{2,j}^{d_2} \cdot \ldots \cdot Q_{m,j}^{d_m} \mod p_j$ for $j = 1, \ldots, f$, wherein $Q_{i,j} = Q_i \mod p_j$ for $i = 1, \ldots, m$ and $j = 1, \ldots, f$; and

determining that the message M is authentic if the response D has a value such that: $h\!\left(M, D^v \cdot G_1^{\varepsilon_1 d_1} \cdot G_2^{\varepsilon_2 d_2} \cdot \ldots \cdot G_m^{\varepsilon_m d_m} \mod n\right)$ is equal to the token T, wherein, for $i = 1, \ldots, m$, $\varepsilon_i = +1$ in the case $G_i \cdot Q_i^v = 1 \mod n$ and $\varepsilon_i = -1$ in the case $G_i = Q_i^v \mod n$.

36. (New) The computer readable medium according to claim 32, wherein the challenges are such that $0 \le d_i \le 2^k - 1$ for $i = 1, \ldots, m$.

37. (New) The computer readable medium according to claim 33, wherein the challenges are such that $0 \le d_i \le 2^k - 1$ for $i = 1, \ldots, m$.

38. (New) The computer readable medium according to claim 34, wherein the challenges are such that $0 \le d_i \le 2^k - 1$ for $i = 1, \ldots, m$.

39. (New) The computer readable medium according to claim 35, wherein the challenges are such that $0 \le d_i \le 2^k - 1$ for $i = 1, \ldots, m$.

40. (New) A computer readable medium storing instructions which when executed cause a processor to execute the following method:

obtaining a set of one or more private values $Q_1, Q_2, \ldots, Q_m$ and respective public values $G_1, G_2, \ldots, G_m$, each pair of values Q_i, G_i verifying either the equation $G_i \cdot Q_i^v \equiv 1 \mod n$ or the equation $G_i \equiv Q_i^v \mod n$, wherein m is an integer greater than or equal to 1, i is an integer

14

between 1 and m, and wherein n is a public integer equal to the product of f private prime factors designated by $p_1,...,p_f$, at least two of these prime factors being different from each other, wherein f is an integer greater than 1, and wherein v is a public exponent such that $v = 2^k$, and wherein k is a security parameter having an integer value greater than 1, and wherein each public value G_i for $i = 1,...,m$ is such that $G_i \equiv g_i^2 \bmod n$, wherein g_i for $i = 1,...,m$ is a base number having an integer value greater than 1 and smaller than each of the prime factors $p_1,...,p_f$, and g_i is a non-quadratic residue of the ring of integers modulo n;

recording a message M to be signed;

choosing m integers r_i randomly, wherein i is an integer between 1 and m;

computing commitments R_i having a value such that: $R_i = r_i^v \bmod n$ for $i = 1,...,m$;

computing a token T having a value such that $T = h(M, R_1, R_2,..., R_m)$, wherein h is a hash function producing a binary train consisting of m bits;

identifying the bits $d_1, d_2,...,d_m$ of the token T; and

computing responses $D_i = r_i \cdot Q_i^{d_i} \bmod n$ for $i = 1,...,m$.

41.   (New) The computer readable medium according to claim 40, the method further comprising:

collecting the token T and the responses D_i for $i = 1,...,m$; and

15

U.S. Patent Application Serial No. 09/889,918
Reply to Office Action dated May 16, 2006

determining that the message M is authentic if the response D has a value such that:

$h\left(M, D^{v} \cdot G_{1}^{\varepsilon_{1} d_{1}} \cdot G_{2}^{\varepsilon_{2} d_{2}} \cdot \ldots \cdot G_{m}^{\varepsilon_{m} d_{m}} \mod n\right)$ is equal to the token T, wherein, for $i = 1, \ldots, m$,

$\varepsilon_{i} = +1$ in the case $G_{i} \cdot Q_{i}^{v} = 1 \mod n$ and $\varepsilon_{i} = -1$ in the case $G_{i} = Q_{i}^{v} \mod n$.

16